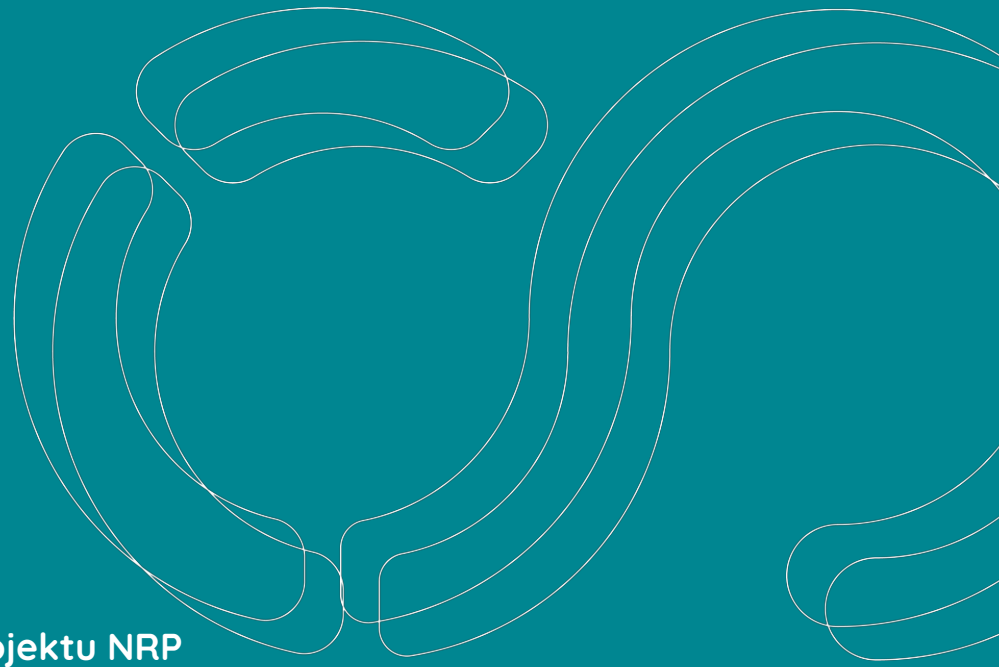
National Czech Programme | eosc

Kybernetická bezpečnost a odolnost proti vlivovému působení cizí moci v EOSC CZ

Jan Kolouch



Spolufinancováno Evropskou unií

Ministerstvo školství, mládeže a tělovýchovy

cesnet

Registrační číslo projektu NRP
CZ.02.01.01/00/23_014/0008787

National Czech Programme | eosc

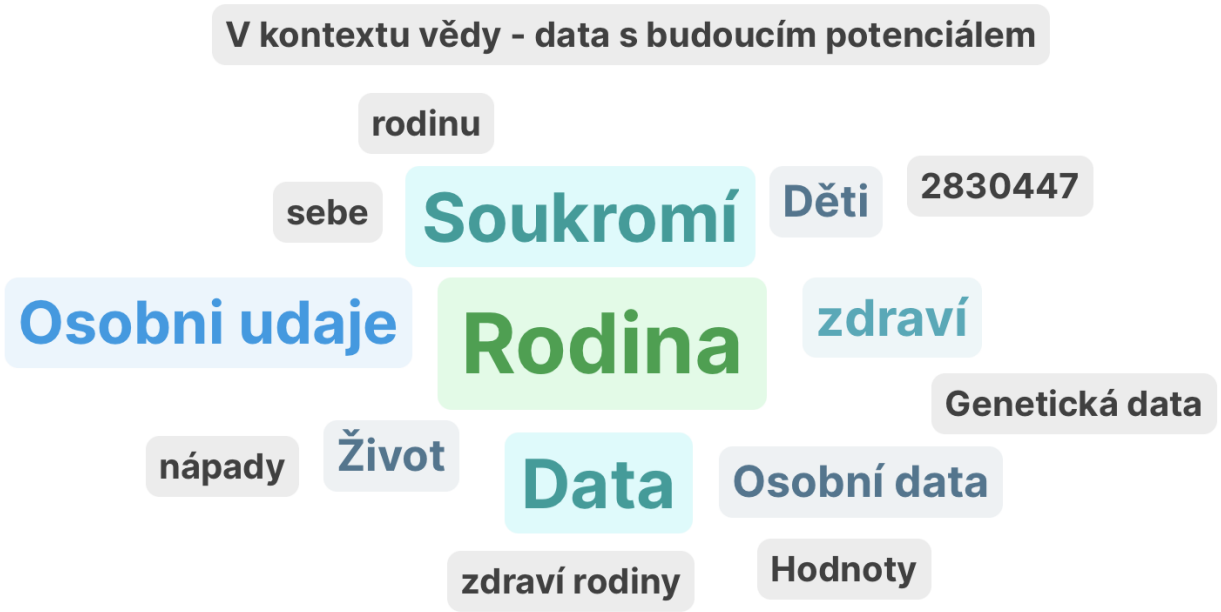
Co je pro vás to nejcennější, co chcete chránit?

Slido.com

2830447

Co je pro vás to nejcennější, co chcete chránit?

Review answers 20 >



National Czech Programme | eosc

Co považujete za nejcennější/nejhodnotnější aktivum Vaší organizace?

Slido.com

2830447

Co považujete za nejcennější/nejhodnotnější aktivum Vaší organizace?

Review answers 28

Kybernetická kriminalita 3. největší ekonomika světa (2025)

Cybercrime The World's Third Largest Economy After the U.S. and China

Stu Sjouwerman

Tweet Share

Cybersecurity Ventures released a new report that showed cybercrime is going to cost the world $8 trillion USD in 2023.

If it were measured as a country, then cybercrime would be the world's third largest economy after the U.S. and China.

"We expect global cybercrime damage costs to grow by 15 percent per year over the next three years, reaching $10.5 trillion USD annually by 2025, up from $3 trillion USD in 2015.

"Cybercrime costs include damage and destruction of data, stolen money, lost productivity, theft of intellectual property, theft of personal and financial data, embezzlement, fraud, post-attack disruption to the normal course of business, forensic investigation, restoration and deletion of hacked data and systems, and reputational harm."

https://blog.knowbe4.com/cybercrime-the-worlds-third-largest-economy-after-the-u.s.-and-china

Kyberútoky na české univerzity nejsou neobvyklé. Motivací je výpalné, data i patenty

2. říjen 2023 | Antivirus

https://radiozurnal.rozhlas.cz/kyberutoky-na-ceske-univerzity-nejsou-neobvykle-motivaci-je-vypalne-data-i-9083939

National Czech Programme

Školy a univerzity stále více doplácejí na zanedbávání zranitelností

3. 9. 2024. (redaktor: František Doupal, zdroj: Sophos)

Školy a univerzity jsou stále jedním z hlavních cílů kybernetických útoků, včetně ransomwaru. Podle výroční zprávy společnosti Sophos se navzdory poklesu počtu útoků dramaticky zvýšily náklady spojené s jejich odražením a obnovou.

V roce 2023 se 63 % škol a 66 % univerzit na celém světě stalo obětí útoků ransomwaru. Ačkoli je to menší procento než v roce 2022, kdy činilo 80 %, respektive 79 %, náklady na obnovu dat prudce vzrostly. Průměrné náklady na obnovu dat po ransomwarovém útoku v institucích nižšího vzdělávání se více než zdvojnásobily na 3,76 milionu dolarů, zatímco na univerzitách jde o téměř čtyřnásobný nárůst na 4,02 milionu dolarů.

Jedním z nejvíce alarmujících zjištění průzkumu je, že 95 % vzdělávacích institucí, které loni zažily útok, zaznamenalo pokusy kyberzločinců o narušení bezpečnosti záloh. Bohužel více než 70 % těchto pokusů bylo úspěšných. Kromě toho 85 % útoků na školy a 77 % bezpečnostních narušení na univerzitách vedlo k zašifrování dat, což je nárůst oproti výsledkům průzkumu z roku 2023, tedy případům zašifrování v roce 2022.

https://www.rmol.cz/novinky/skoly-univerzity-stale-vice-doplaceji-na-zanedbavani-zranitelnosti

zd_KORNDGQGJKME.docx

- Avšak **právě vzdělávací a výzkumné instituce představují subjekty, které dlouhodobě čelí vyššímu počtu kybernetických útoků**.
- Zahrnutí tohoto odvětví do nové regulace je tudíž logickým a zároveň nezbytným krokem, neboť **vědu, výzkum a vzdělávání lze označit za oblasti, které mají zásadní celospolečenský význam a jejich dnes již z většiny digitalizovaná data jsou předmětem jak kybernetické, tak klasické špionáže** ať již motivované zájmy států či prostým finančním ziskem.

Proč jsou univerzity stále častěji terčem kyberútoků?

332,3/den

4/den

Út…achem digitál…
te… útoky probíha…
ni… dlouho cíl n…
všimnout, případně … nich ani nemusí dozvědět. Pokud nějaký velký útok proběhne … lokdy se tyto případy dostanou do médií a do povědomí širok… řejnosti. Věděli jste například, že Masarykova univerz… elí takovým útokům v podstatě denně?

24.4.2023

121 290

Pokusů o kybernetický útok

1494

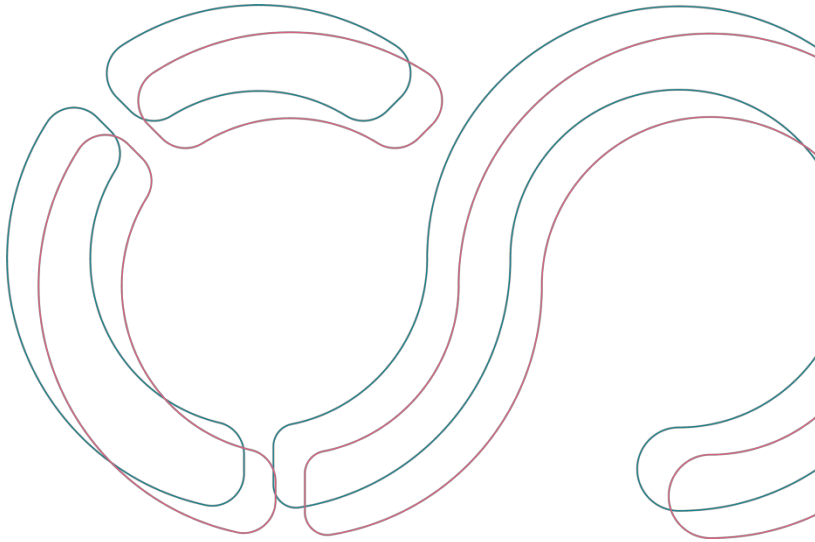
Incidentů řešeno manuálně

200%

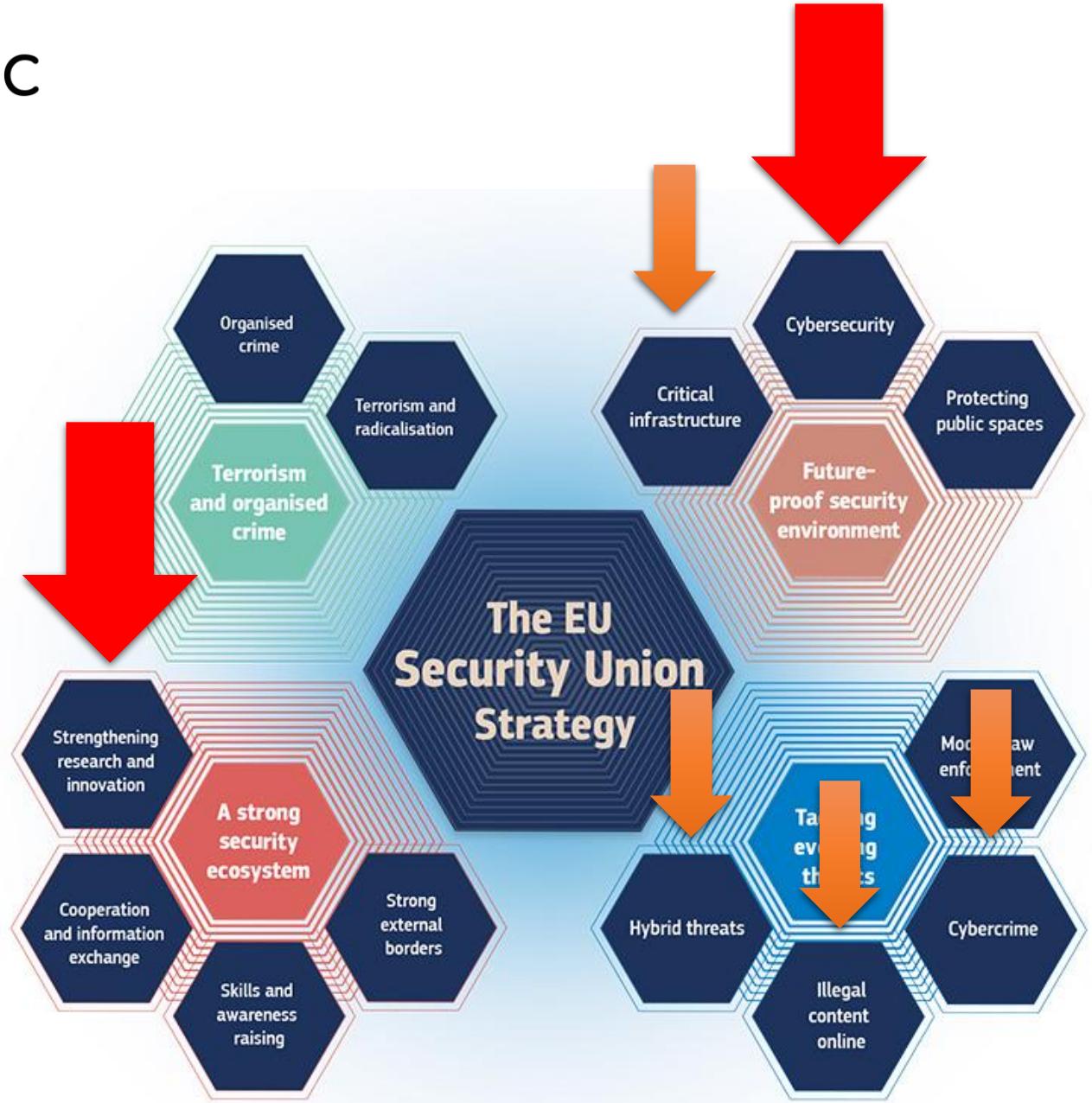
Nárůst oproti roku 2019

https://security.muni.cz/clanky/proc-jsou-univerzity-stale-casteji-tercem-kyberutoku

Jen hasit požáry už nestačí…

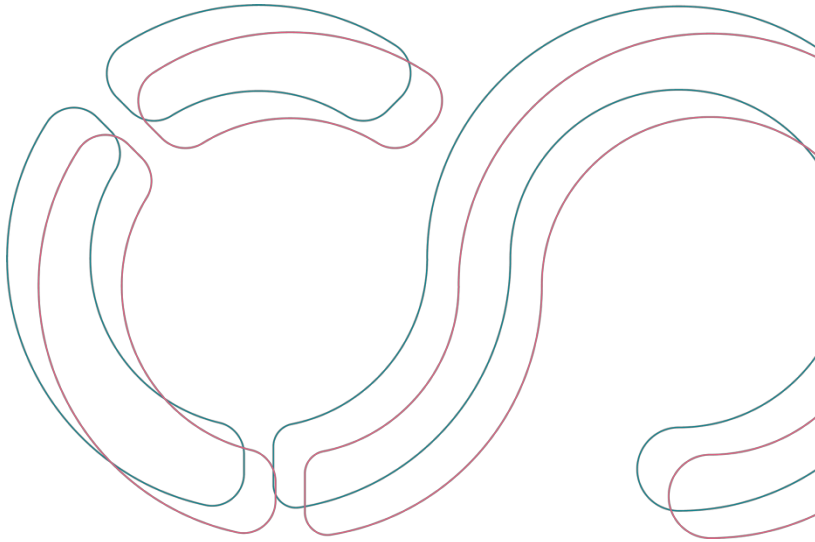


2021



https://cclab.com/news-details/european-union-to-regulate-it-security-of-critical-infrastructures/106

Kybernetická bezpečnost



Novum?

- **Směrnice** Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 **o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Uni (NIS 1)**
- **Zákon č. 181/2014 Sb., o kybernetické bezpečnosti**
- **Vyhláška č. 82/2018 Sb.,** o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška **o kybernetické bezpečnosti**)

NIS 2

- ~~**Směrnice** Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022 **o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii** a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148 **(směrnice NIS 2)**~~

- **Zákon č. 264/2025 Sb., o kybernetické bezpečnosti**

Vyhlášky

- **408/2025 Sb., o regulovaných službách**

  https://www.e-sbirka.cz/sb/2025/408?zalozka=text

- **409/2025** Sb., o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností

  https://www.e-sbirka.cz/sb/2025/409?zalozka=text

- **410/2025** Sb., o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností

  https://www.e-sbirka.cz/sb/2025/410?zalozka=text

- **411/2025** Sb., o bezpečnostních úrovních informačních systémů veřejné správy

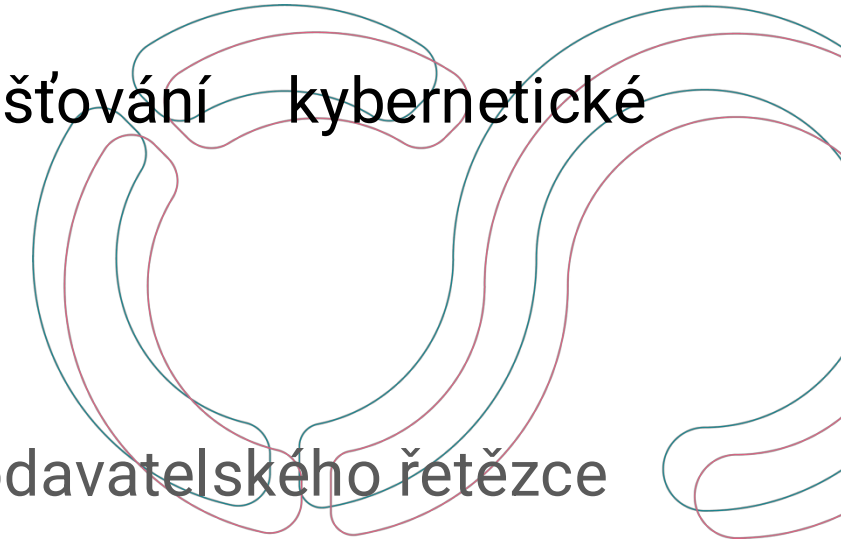
  https://www.e-sbirka.cz/sb/2025/411?zalozka=text

- **412/2025** Sb.,o bezpečnostních pravidlech pro orgány veřejné správy využívající služby poskytovatelů cloud computingu

  https://www.e-sbirka.cz/sb/2025/412?zalozka=text

Hlavní změny

- **Rozšíření počtu povinných osob**
- **Změna způsobu identifikace** povinných osob
- Doplnění **nových požadavků na zavádění bezpečnostních opatření**
- Doplnění **nových požadavků na proces hlášení kybernetických bezpečnostních incidentů**
- **Větší odpovědnost vrcholného vedení** za zajišťování kybernetické bezpečnosti
- **Větší důraz na sdílení informací**
- **Zvýšení pokut** a nové formy správního trestání
- Nové požadavky na řešení problematiky bezpečnosti dodavatelského řetězce



https://portal.nukib.gov.cz/

Odvětví regulovaných služeb

https://portal.nukib.gov.cz/informacni-servis/podpurne-materialy/67b316bdc3c48e2492025682

National Czech Programme | eosc

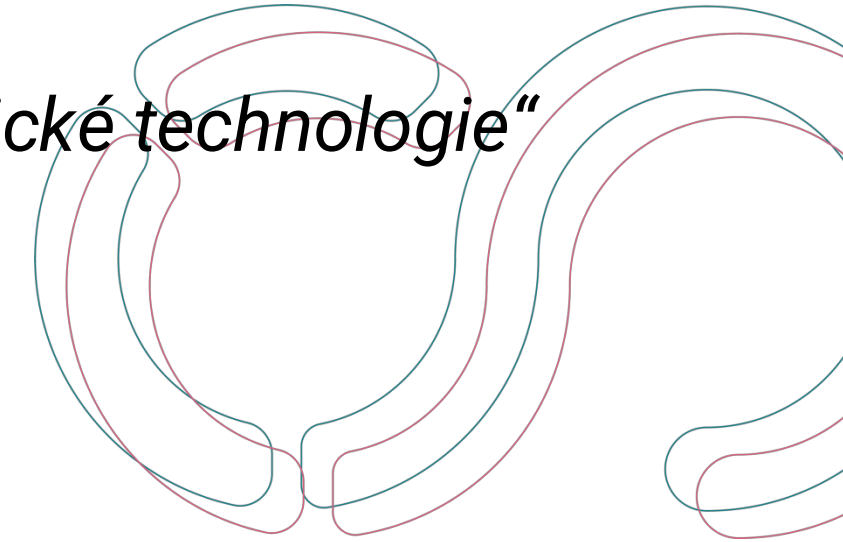
Vyhláška č. 408/2025 Sb., o regulovaných službách

Regulovaná služba

Služba	Podmínky významnosti poskytovatele regulované služby a jeho režim
19.1 Výzkum a vývoj	Veřejná výzkumná instituce[49)], výzkumná organizace podle přímo použitelného předpisu Evropské unie[50)], **vysoká škola** nebo výzkumná instituce, kterou se rozumí osoba, jejímž hlavním cílem je provádět aplikovaný výzkum[51)] za účelem využití výsledků tohoto výzkumu pro komerční účely, která není vzdělávací institucí, je **I. poskytovatelem regulované služby v režimu vyšších povinností v případě, že** **a) v posledních 5 kalendářních letech prováděla alespoň 2 kalendářní roky citlivou výzkumnou činnost**, kterou se rozumí **činnost zaměřená na aplikovaný výzkum vojenského materiálu** uvedeného v seznamu vojenského materiálu podle zákona o zahraničním obchodu s vojenským materiálem[52)], **nebo** **b) v posledních 5 kalendářních letech prováděla alespoň 2 kalendářní roky aplikovaný výzkum technologie spadající do některé z následujících technologických oblastí** podle doporučení Komise o technologických oblastech s kritickým významem pro hospodářskou bezpečnost EU[53)]: **1. technologie pokročilých polovodičů,** **2. technologie umělé inteligence,** **3. kvantové technologie, nebo** **4. biotechnologie, nebo** II. poskytovatelem regulované služby v režimu nižších povinností v případě, že v posledních 5 kalendářních letech prováděla alespoň 2 kalendářní roky aplikovaný výzkum technologie spadající do některé z následujících technologických oblastí podle doporučení Komise o technologických oblastech s kritickým významem pro hospodářskou bezpečnost EU[53)]: **1. pokročilá konektivita, navigace a digitální technologie,** **2. technologie pokročilého snímání,** **3. vesmírné technologie a technologie pohonu,** **4. energetické technologie,** **5. robotika a autonomní systémy, nebo** **6. pokročilé materiály, výrobní a recyklační technologie.** **Výzkumná instituce je poskytovatelem regulované služby v režimu nižších povinností v případě, že je velkým nebo středním podnikem.**

Základní podmínky

- **Aplikovaný výzkum (citlivá výzkumná činnost)**
- **Časové kritérium** – v posledních **5 kalendářních letech** musí instituce provádět tento výzkum **alespoň 2 roky**
- **Předmět výzkumu:** vojenský materiál nebo *„kritické technologie“*



Aplikovaný výzkum

Pojem **aplikovaný výzkum** obsažený v definici výzkumné instituce nahrazuje směrnicí NIS2 použité sousloví „*aplikovaný výzkum nebo experimentální vývoj*“, které vychází z manuálu Frascati z roku 2015 vypracovaného Organizací pro hospodářskou spolupráci a rozvoj. Aplikovaný výzkum je v návaznosti na manuál Frascati a sdělení Komise o rámci pro státní podporu výzkumu, vývoje a inovací ze dne 28. října 2022 (2022/C 414/01) **definován v § 2 odst. 1 písm. b) zákona č. 130/2002 Sb. jako**

„teoretická a experimentální práce zaměřená na získání nových poznatků a dovedností pro vývoj nových nebo podstatně zdokonalených výrobků, postupů nebo služeb; průmyslový výzkum, experimentální vývoj nebo jejich kombinace jsou součástí aplikovaného výzkumu“.

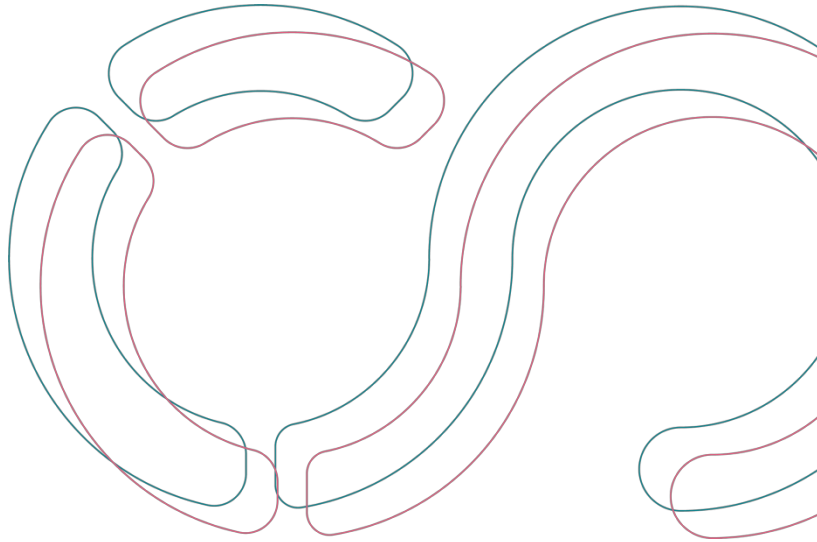
Aplikovaný výzkum – z.č. 328/2025 Sb.

§ 2 odst. 1 písm. b) zákona č. 130/2002 Sb. jako

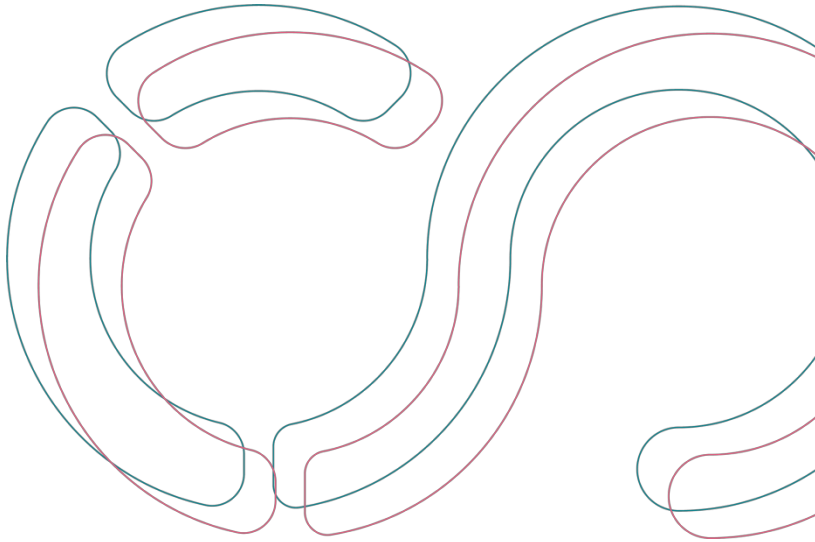
„aplikovaným výzkumem průmyslový výzkum podle přímo použitelného předpisu Evropské unie upravujícího blokové výjimky[3]), experimentální vývoj podle přímo použitelného předpisu Evropské unie upravujícího blokové výjimky[4]) nebo jejich kombinace, “.

Citlivá výzkumná činnost

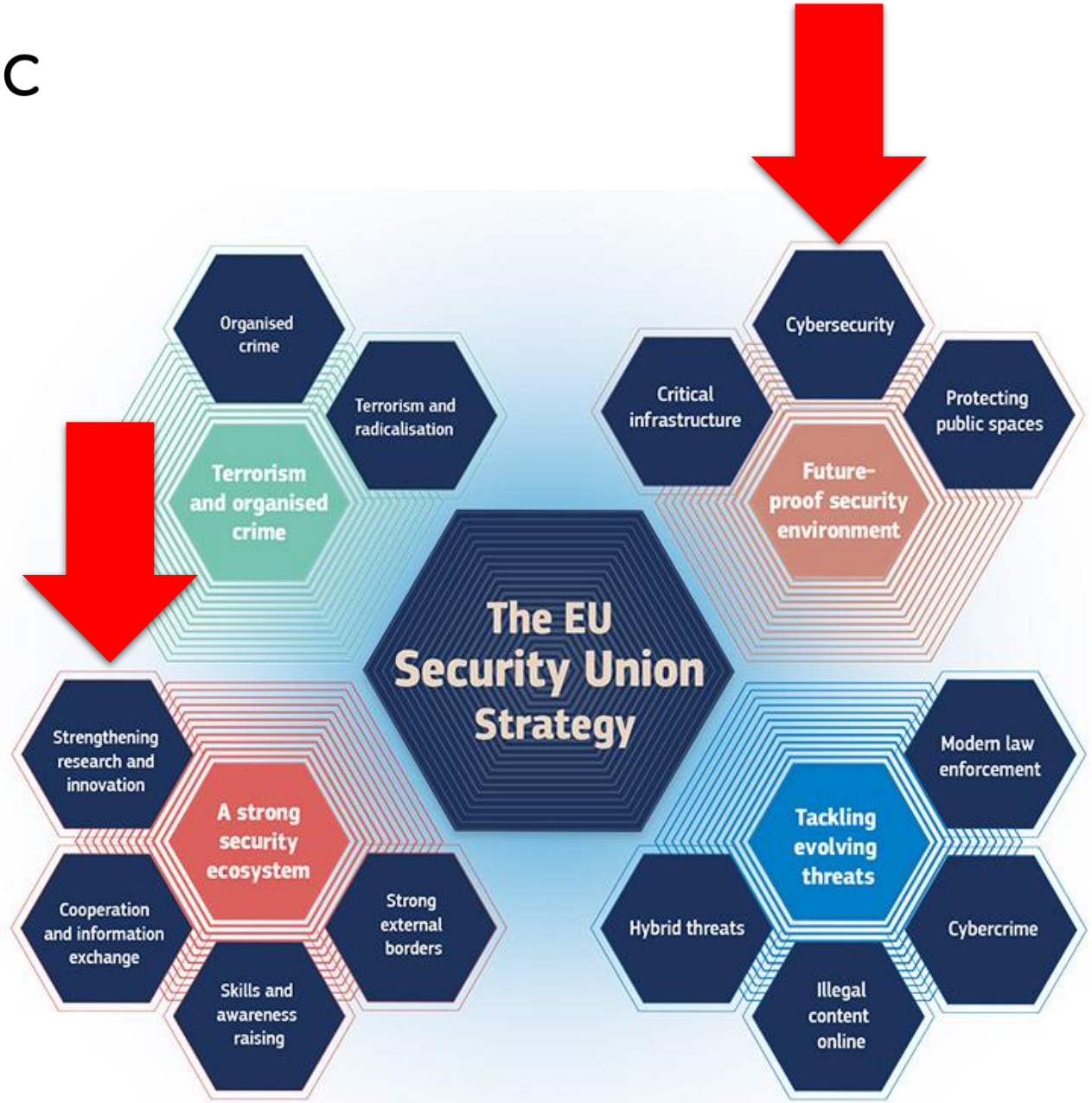
Citlivá výzkumná činnost se tak týká těch organizací, které se **zabývají výzkumem vojenského materiálu uvedeného v seznamu vojenského materiálu** podle zákona č. 38/1994 Sb., o zahraničním obchodu s vojenským materiálem.



Provázání s institucionální odolností



2021



https://cclab.com/news-details/european-union-to-regulate-it-security-of-critical-infrastructures/106

National Czech Programme | eosc

European Commission

EN

Defence Industry and Space

Home | Newsroom | EU Space | EU Defence Industry | EU Aeronautics Industry | Support to Ukraine | Funding opportunities

Home > Commission Recommendation of 03 October 2023 on critical technology areas for the EU's economic security for further risk assessment with Member States

Commission Recommendation of 03 October 2023 on critical technology areas for the EU's economic security for further risk assessment with Member States

RECOMMENDATION

https://defence-industry-space.ec.europa.eu/commission-recommendation-03-october-2023-critical-technology-areas-eus-economic-security-further_en

National Czech Programme | eosc

Bezpečnost výzkumu – posilování odolnosti vůči nelegitimnímu ovlivňování

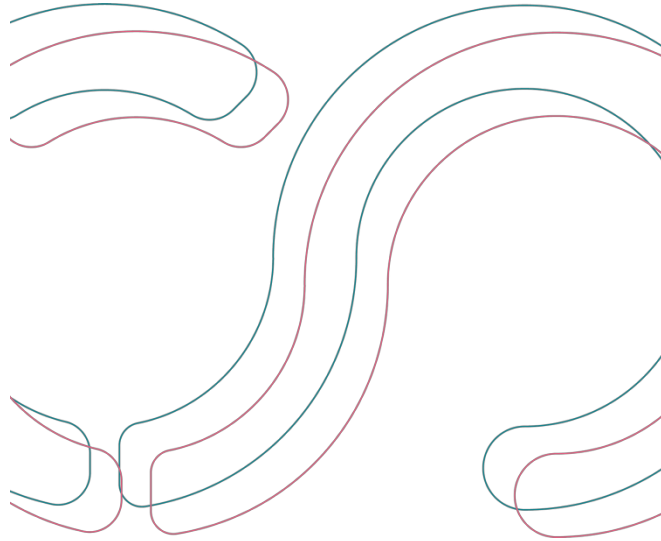
BEZPEČNOST VÝZKUMU – POSILOVÁNÍ ODOLNOSTI VŮČI NELEGITIMNÍMU OVLIVŇOVÁNÍ

MŠMT dne 17. června 2024 představilo v rámci odborného semináře soubor dokumentů, který přispěje ke zvyšování odolnosti vůči nelegitimnímu ovlivňování ve vysokoškolském a výzkumném prostředí.

Mezirezortní pracovní skupiny pro potírá[illegible]nelegitimního ovlivňování ve vysoko[illegible]olském a výzkum[illegible]m prostředí se zásadním přispěním Ministerstva školství mládeže a tělovýchovy, Ministerstva vnitra a Akademie věd ČR a v konzultaci se zástupci dalších českých vysokoškolských a výzkumných institucí předkládá soubor dokumentů ke zvyšování odolnosti vůči nelegitimnímu ovlivňování ve vysokoškolském a výzkumném prostředí. Uvedený soubor dokumentů byl vypracován ve snaze o zamezení tříštivého přístupu relevantních institucí k problematice nelegitimního ovlivňování.

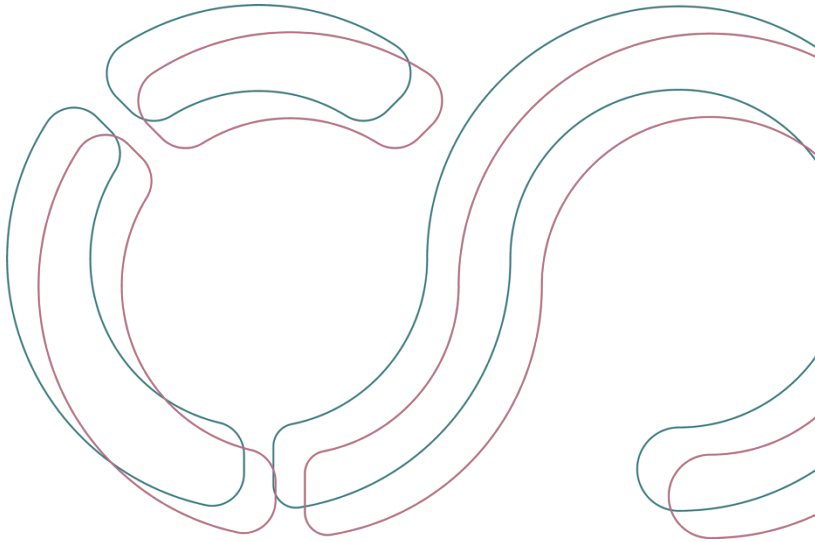
Metodicke_doporuceni_due_diligence_a_rizeni_rizik_spoluprace
Metodicke_doporuceni_k_rizeni_rizik_bezpecnosti_vyzkumu_na_institucionalni_urovni
Posilovani_odolnosti_vuci_nelegitimnimu_ovlivnovani_ve_vysokoskolskem_a_vyzkumnem_prostredi

https://msmt.gov.cz/vyzkum-a-vyvoj-2/bezpecnost-vyzkumu-posilovani-odolnosti-vuci-nelegitimnimu



TECHNOLOGICKÁ OBLAST	* Technologie uvedené u každé oblasti představují pravděpodobné klíčové body pro hodnocení rizik, jejich seznam však není vyčerpávající.
1. POKROČILÉ POLOVODIČOVÉ TECHNOLOGIE	• Mikroelektronika včetně procesorů • Fotonika (včetně vysokoenergetických laserů) • Vysokofrekvenční čipy • Zařízení na výrobu polovodičů ve velmi pokročilých velikostech uzlů
2. TECHNOLOGIE UMĚLÉ INTELIGENCE	• Vysokovýkonná výpočetní technika • Cloud a edge computing • Technologie datové analýzy • Počítačové vidění a zpracování jazyka, rozpoznávání objektů
3. KVANTOVÉ TECHNOLOGIE	• Kvantové výpočty • Kvantová kryptografie • Kvantová komunikace • Kvantové snímání a radary
4. BIOTECHNOLOGIE	• Techniky genetické modifikace • Nové genomické techniky • Genový tah • Syntetická biologie
5. POKROČILÁ KONEKTIVITA, NAVIGACE A DIGITÁLNÍ TECHNOLOGIE	• Zabezpečená digitální komunikace a konektivita, jako např. RAN a otevřená RAN (rádiová přístupová síť) a 6G • Technologie pro kybernetickou bezpečnost včetně kybernetického dohledu, bezpečnostních systémů a systémů proti vniknutí, digitální forenzní analýzy • Internet věcí a virtuální realita • Technologie distribuované účetní knihy a digitální identity • Naváděcí, navigační a řídící technologie včetně avioniky a určování polohy na moři
6. POKROČILÉ SNÍMACÍ TECHNOLOGIE	• Elektrooptické, radarové, chemické, biologické, radiační a distribuované snímání • Magnetometry, magnetické gradiometry • Podvodní snímače elektrického pole • Gravimetry a gradiometry
7. VESMÍRNÉ A POHONNÉ TECHNOLOGIE	• Technologie specializující se na vesmír od úrovně jednotlivých součástí po celý systém • Technologie pro sledování vesmíru a pozorování Země • Určování polohy, navigace a času ve vesmíru (PNT) • Zabezpečená komunikace včetně připojení na nízkou oběžnou dráhu Země (LEO) • Pohonné technologie včetně hypersoniky a součástí pro vojenské použití
8. ENERGETICKÉ TECHNOLOGIE	• Technologie jaderné fúze, reaktory a výroba elektrické energie, technologie radiologické přeměny/obohacování/recyklace • Vodíková a nová paliva • Net-zero technologie včetně fotovoltaiky • Inteligentní sítě a uchovávání energie, baterie
9. ROBOTIKA A AUTONOMNÍ SYSTÉMY	• Drony a vozidla (vzdušné, pozemní, povrchové a podvodní) • Roboti a roboticky řízené přesné systémy • Exoskelety • Systémy s podporou AI
10. POKROČILÉ MATERIÁLY, VÝROBNÍ A RECYKLAČNÍ TECHNOLOGIE	• Technologie pro nanomateriály, chytré materiály, pokročilé keramické materiály, stealth materiály, materiály navržené jako bezpečné a udržitelné • Aditivní výroba včetně výroby v terénu (mimo výrobní závod) • Digitálně řízená výroba s mikropřesností a laserové obrábění/svařování v malém měřítku • Technologie pro těžbu, zpracování a recyklaci kritických surovin (včetně hydrometalurgické těžby, biologického loužení, filtrace pomocí nanotechnologie, elektrochemického zpracování a černé hmoty)

Společný jmenovatel

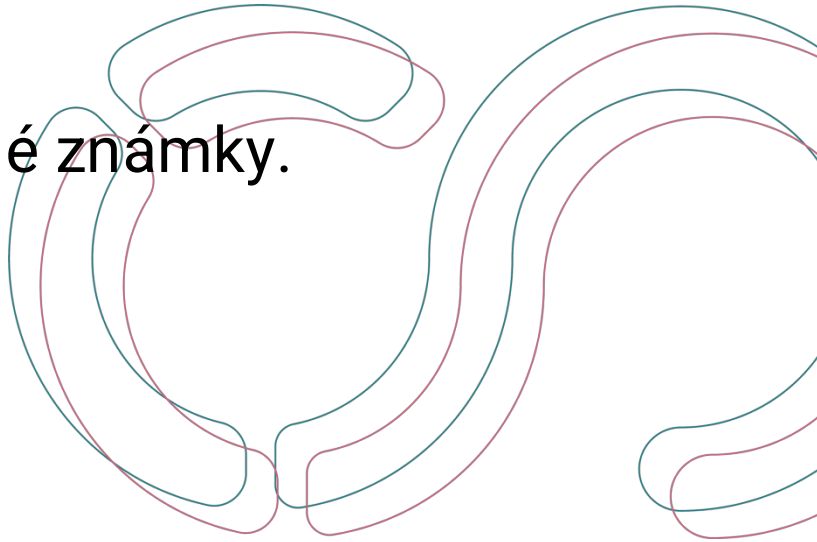


Aktivum

Cokoliv co má pro mě hodnotu…

Typicky:

- **Fyzická aktiva:** Budovy, stroje, pozemky, zásoby.
- **Finanční aktiva:** Akcie, dluhopisy, peníze na účtu
- **Nehmotná aktiva:** Patenty, licence, software, ochranné známky.
- **Další aktiva:** **Informace**, data, zaměstnanci, **služby**.

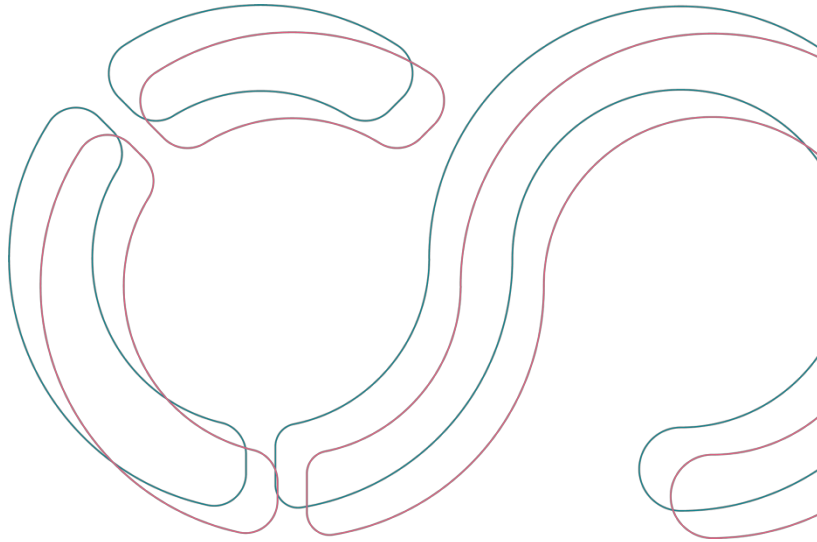


https://google.com/cojetoaktivum

Aktivum dle § 2 odst. 1 písm. c) ZoKB

- ***fyzický*** *nebo* ***digitální prostředek***, ***osoba*** *nebo* ***činnost*** ***související se zpracováváním informací a dat v elektronické podobě“***

- Rozdělení:
  - **Primární aktivum** § 2 odst. 1 písm. d) NZoKB
  - **Podpůrné aktivum** § 2 odst. 1 písm. e) NZoKB



Primární aktivum

*„aktivum v podobě **zpracovávané informace** nebo **poskytované služby** “*

- **Zpracovávaná informace:** **veškeré informace, se kterými organizace nakládá** (např. o informace zpracovávané a vytvořené v rámci chodu organizace a poskytování služeb, provozu informačních a komunikačních systémů (včetně logů a metadat), záznamy o provozu, data o uživatelích, osobní údaje, přístupové údaje, data relací, konfigurační soubory, zdrojové kódy, zálohy, certifikáty apod.)
- **Poskytovaná služba:** **vykonávání jednotlivých činností organizace**, získávání, poskytování, zpracování, shromažďování, vyhodnocování, ukládání, předávání, likvidování informací včetně jejich zobrazení, umožnění komunikace, zajištění elektronické pošty, atd.

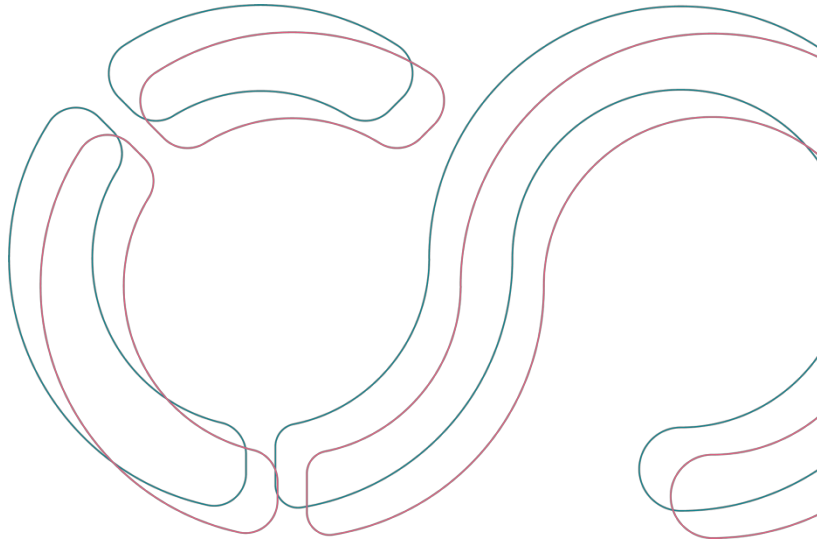
Co vše?

- Zákon nestanovuje konkrétní úroveň granularity toho, co informací nebo službou je.
- **Primárním aktivem může být:**
  - **„zajištění IS na VŠ“**
  - **„činnost senzoru v trhací jámě č. 1“**

- **Cíl = nastavit úroveň** granularity, **tak aby byla** v případě dostatečně **vypovídající a vhodná pro systematické zavádění kybernetické bezpečnosti**.

Podpůrné aktivum

„aktivum zajišťující fungování primárních aktiv, ***zejména zaměstnanec****,* ***dodavatel****,* ***technické aktivum****,* ***budova*** *a* ***jiný ohraničený prostor****, ve kterém se nachází aktivum regulované služby“*



Aktiva

§ 12

Stanovení rozsahu řízení kybernetické bezpečnosti

(1) Součástí rozsahu řízení kybernetické bezpečnosti (dále jen „stanovený rozsah“) jsou aktiva související s poskytováním regulované služby.

(2) Za účelem vymezení stanoveného rozsahu poskytovatel regulované služby

a) určí všechna svá primární aktiva,

b) **posoudí, zda** primární aktiva **souvisí s poskytováním regulované služby**, a

c) **u primárních** aktiv podle písmene b) **určí podpůrná aktiva**.

Bezpečnost

„***Bezpečnost není produkt, ale proces.***

Je to víc než navrhnout silnou kryptografii do systému; je to o tom navrhnout celý systém tak, aby všechna bezpečnostní opatření, včetně kryptografie, spolupracovala.“

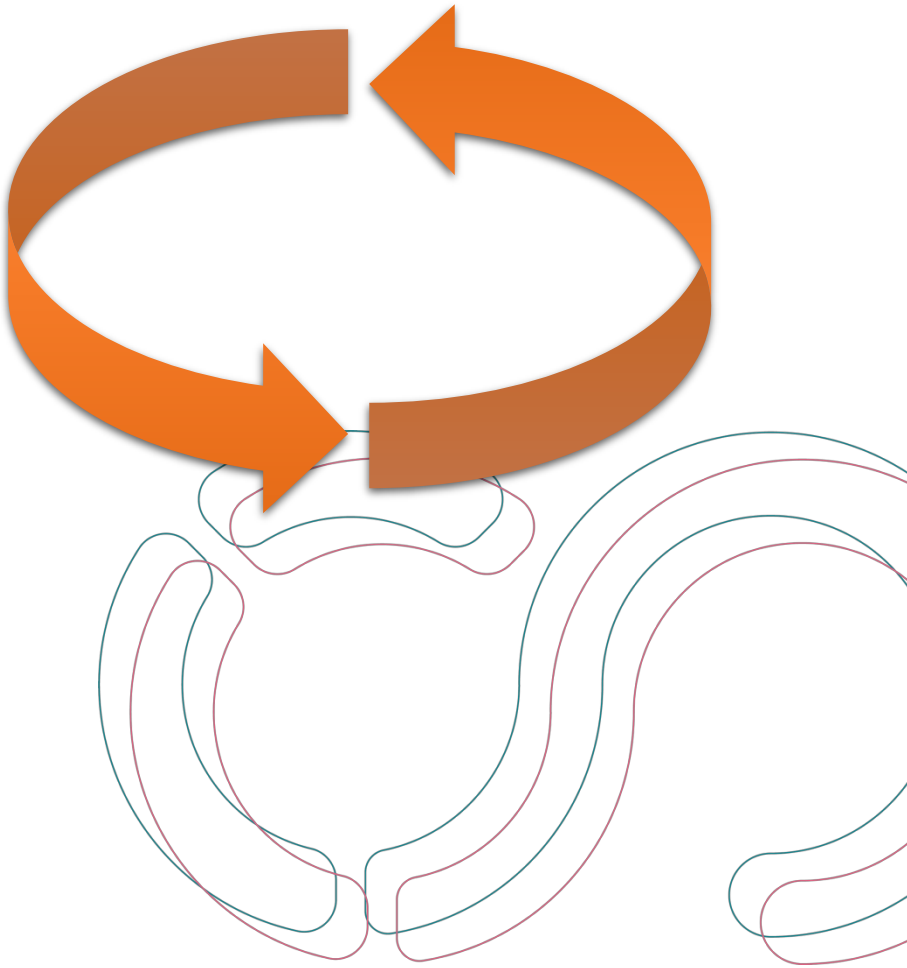
Bruce Schneier

Kdo je zodpovědný?

Vedení

Manažer kybernetické bezpečnosti.

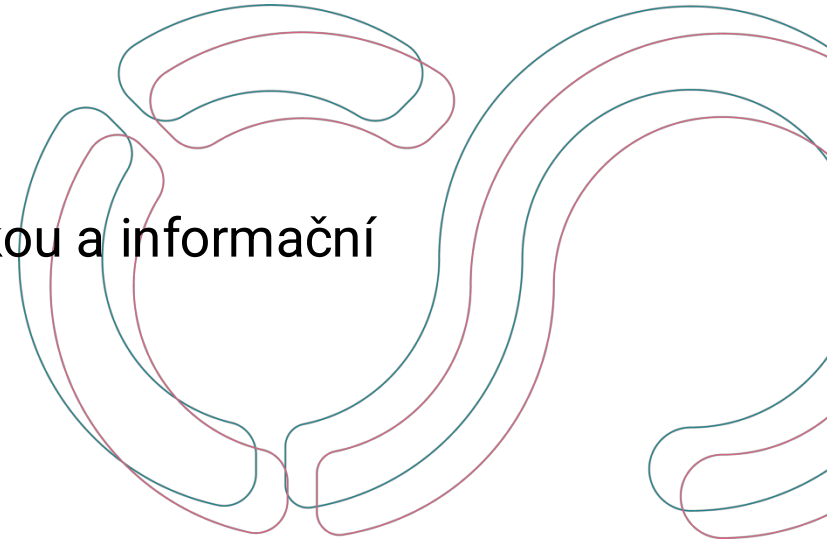
Každý uživatel při „významné“ změně!



Hlavní povinnosti dle ZoKB

V případě **všech poskytovatelů regulované služby**

1. Ohlásit regulovanou službu
2. Hlásit kontaktní údaje
3. **Stanovit rozsah řízení kybernetické bezpečnosti**
4. **Zavádět bezpečnostní opatření**
5. **Hlásit kybernetické bezpečnostní incidenty**
6. **Informovat uživatele o incidentech a hrozbách**
7. **Zavádět protiopatření** vydaná Národním úřadem pro kybernetickou a informační bezpečnost



Zavádění bezpečnostních opatření

Podstatou je zvolit a zavést v organizaci takové procesy a kroky, které pomohou zodolnit organizaci tak, že její služba bude fungovat a bude bezpečná.

Pro poskytovatele regulované služby v režimu vyšších povinností jsou

Organizační opatření

a) systém řízení bezpečnosti informací,
b) povinnosti vrcholného vedení,
c) bezpečnostní role,
d) řízení bezpečnostní politiky a bezpečnostní dokumentace,
e) řízení aktiv,
f) řízení rizik,
g) řízení dodavatelů,
h) bezpečnost lidských zdrojů,
i) řízení změn,
j) akvizice, vývoj a údržba,
k) řízení přístupu,
l) zvládání kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů,
m) řízení kontinuity činností a
n) audit kybernetické bezpečnosti

Technickými opatření

a) fyzická bezpečnost,
b) bezpečnost komunikačních sítí,
c) správa a ověřování identit,
d) řízení přístupových oprávnění,
e) detekce kybernetických bezpečnostních událostí,
f) zaznamenávání bezpečnostních a relevantních provozních událostí,
g) vyhodnocování kybernetických bezpečnostních událostí,
h) aplikační bezpečnost,
i) kryptografické algoritmy,
j) zajišťování dostupnosti regulované služby a
k) zabezpečení průmyslových, řídicích a obdobných specifických technických aktiv.

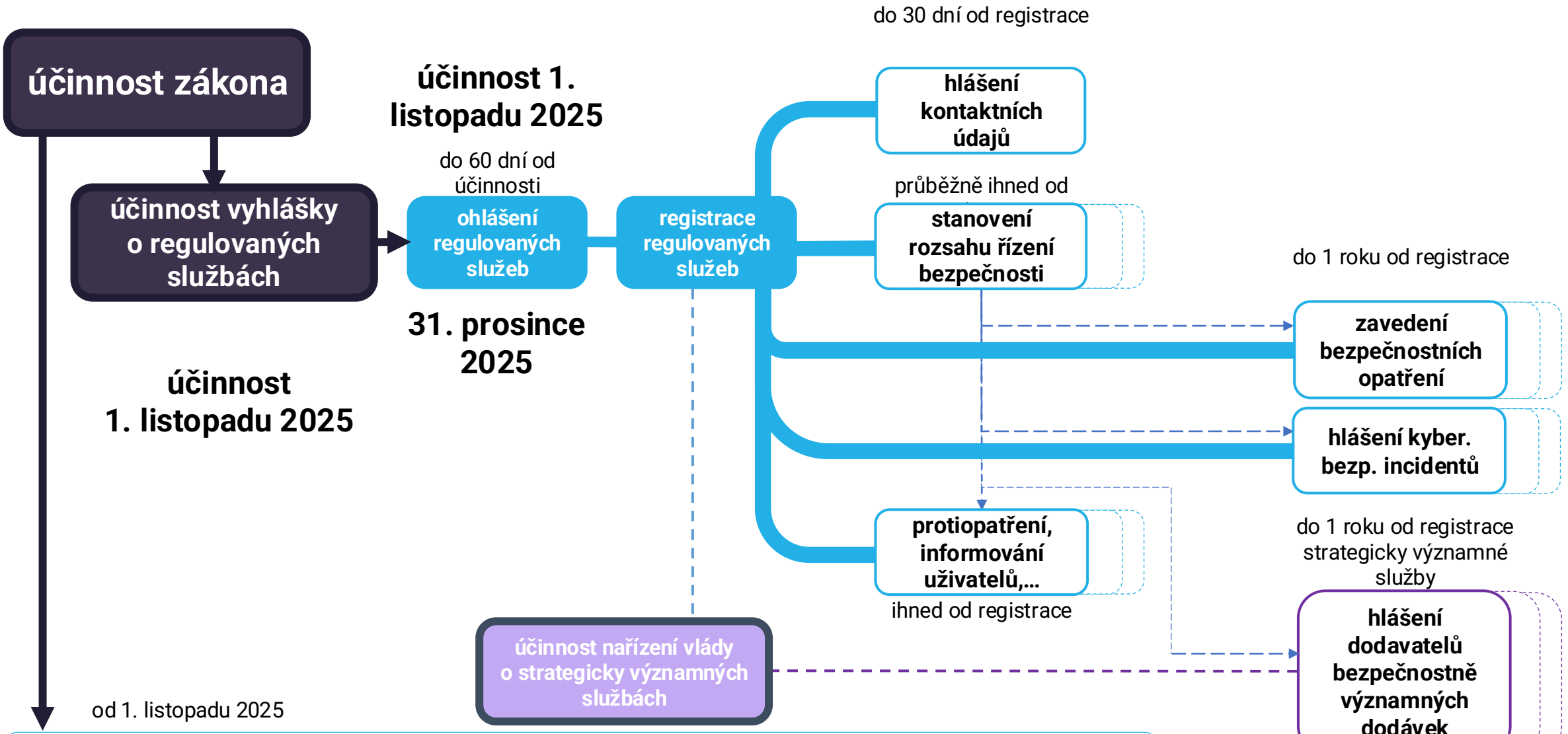
Pro poskytovatele regulované služby v režimu nižších povinností jsou bezpečnostními opatřeními

Organizační a technická opatření

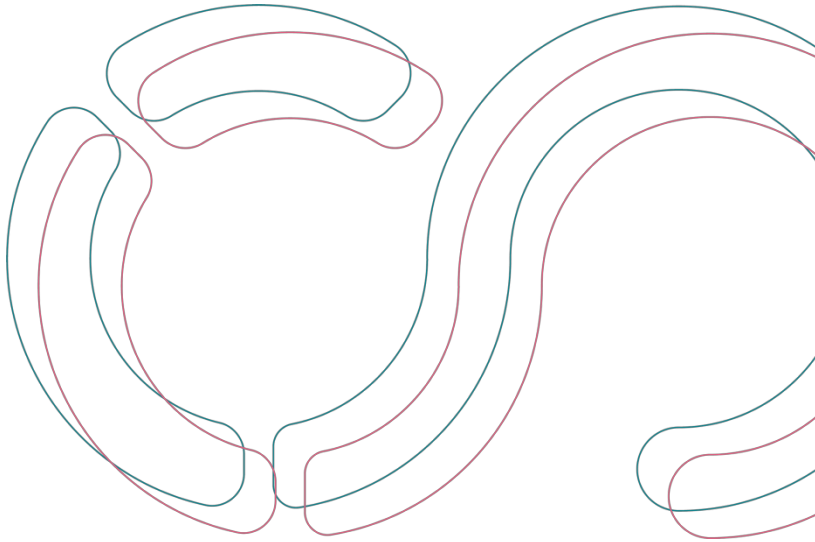
a) systém zajišťování minimální kybernetické bezpečnosti,
b) požadavky na vrcholné vedení,
c) řízení aktiv,
d) řízení rizik,
e) bezpečnost lidských zdrojů,
f) řízení kontinuity činností,
g) řízení přístupu,
h) řízení identit a jejich oprávnění,
i) detekce a zaznamenávání kybernetických bezpečnostních událostí,
j) řešení kybernetických bezpečnostních incidentů,
k) bezpečnost komunikačních sítí,
l) aplikační bezpečnost a
m) kryptografické algoritmy

Zavádění bezpečnostních opatření

- Vyhodnotím rizika – **provedu analýzu rizik**
- Rizika, která nejsou akceptovatelná musím řešit –stanovím si plán řešení = **plán zvládání rizik**
- K rizikům **namapuji opatření z vyhlášky**
- Pokud nějaké opatření nelze zavést ve lhůtě – zdůvodním proč nejde a stanovím plán do kdy a jak provedu
- **Zavádím opatření podle plánu**, provádím audity…


účinnost zákona
účinnost vyhlášky o regulovaných službách
účinnost 1. listopadu 2025
do 60 dní od účinnosti
ohlášení regulovaných služeb
31. prosince 2025
registrace regulovaných služeb
účinnost 1. listopadu 2025
do 30 dní od registrace
hlášení kontaktních údajů
průběžně ihned od
stanovení rozsahu řízení bezpečnosti
do 1 roku od registrace
zavedení bezpečnostních opatření
hlášení kyber. bezp. incidentů
protiopatření, informování uživatelů,...
ihned od registrace
účinnost nařízení vlády o strategicky významných službách
do 1 roku od registrace strategicky významné služby
hlášení dodavatelů bezpečnostně významných dodávek
od 1. listopadu 2025
další povinnosti a práva ze zákona – např. hlášení údajů tzv. registrátory podle Hlavy III zákona, výkon kontroly apod.

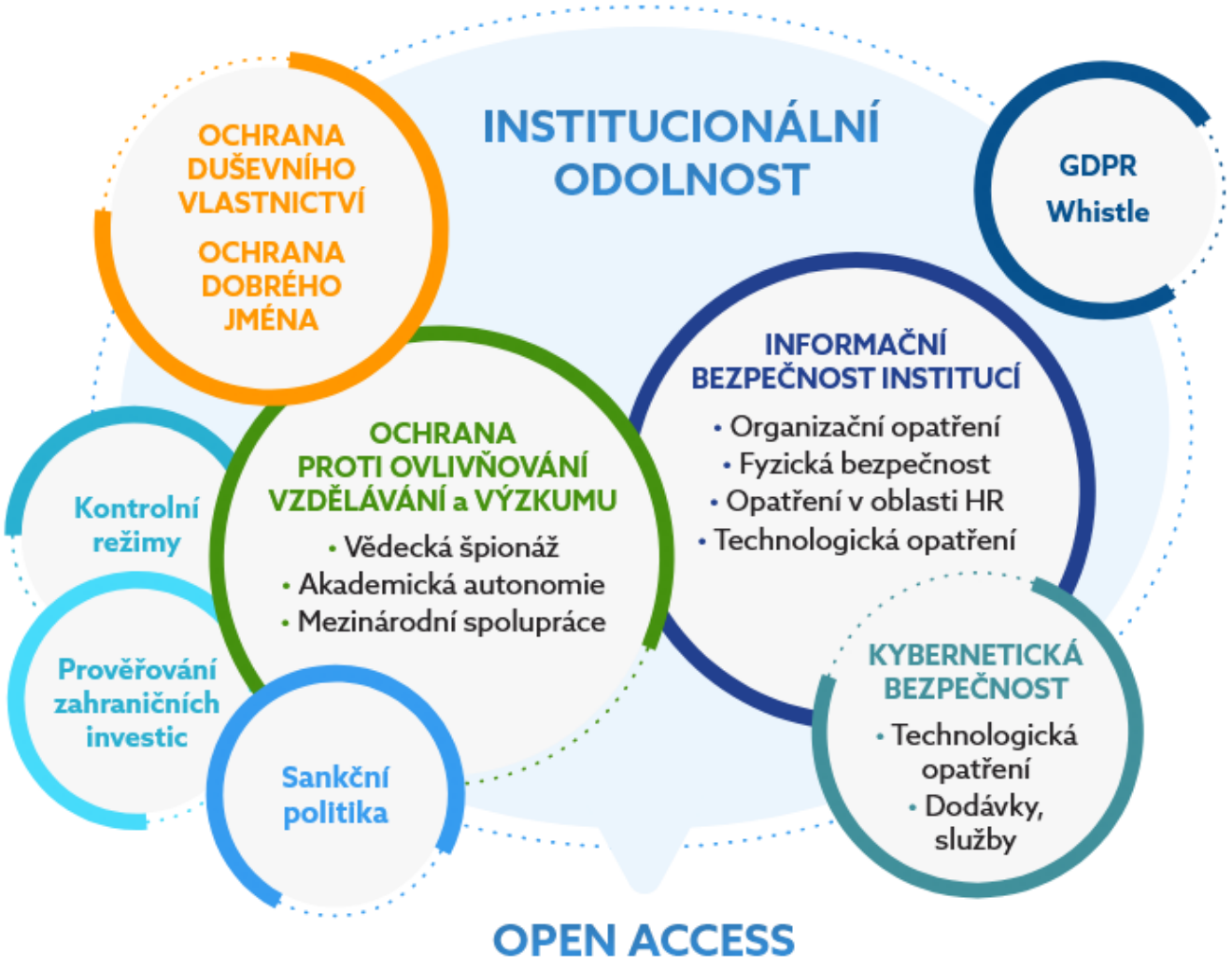
Protivliv
Due diligence
Institucionální odolnost



Důvod a rozsah due diligence

- **Účel náležité péče**
  - Náležitá péče má za **cíl chránit institucionální integritu** a zároveň umožnit **bezpečnou a odpovědnou spolupráci**.
- **Identifikace a zmírňování rizik**
  - Včasná identifikace rizik umožňuje uplatnění ochranných opatření, jako jsou smlouvy, monitorování a kontroly dodržování předpisů.
- **Posilování důvěry a transparentnosti**
  - Bezpečnostní opatření v oblasti výzkumu budují **důvěru a transparentnost pro bezpečnější a udržitelné mezinárodní zapojení**.

Institucionální odolnost



https://msmt.gov.cz/uploads/O31/O311/Bezpecnost_vyzkumu_posilovani_odolnosti_vuci_nelegitimnimu_ovlivnovani/Metodicke_doporuceni_k_rizeni_rizik_bezpecnosti_vyzkumu_na_institucionalni_urovni.pdf

National Czech Programme | eosc

Bezpečnost výzkumu – posilování odolnosti vůči nelegitimnímu ovlivňování

BEZPEČNOST VÝZKUMU – POSILOVÁNÍ ODOLNOSTI VŮČI NELEGITIMNÍMU OVLIVŇOVÁNÍ

MŠMT dne 17. června 2024 představilo v rámci odborného semináře soubor dokumentů, který přispěje ke zvyšování odolnosti vůči nelegitimnímu ovlivňování ve vysokoškolském a výzkumném prostředí.

https://msmt.gov.cz/vyzkum-a-vyvoj-2/bezpecnost-vyzkumu-posilovani-odolnosti-vuci-nelegitimnimu

Mezirezortní pracovní skupiny pro potírání nelegitimního ovlivňování ve vysokoškolském a výzkumném prostředí se zásadním přispěním Ministerstva školství mládeže a tělovýchovy, Ministerstva vnitra a Akademie věd ČR a v konzultaci se zástupci dalších českých vysokoškolských a výzkumných institucí předkládá soubor dokumentů ke zvyšování odolnosti vůči nelegitimnímu ovlivňování ve vysokoškolském a výzkumném prostředí. Uvedený soubor dokumentů byl vypracován ve snaze o zamezení tříštivého přístupu relevantních institucí k problematice nelegitimního ovlivňování.

Metodicke_doporuceni_due_diligence_a_rizeni_rizik_spoluprace
Metodicke_doporuceni_k_rizeni_rizik_bezpecnosti_vyzkumu_na_institucionalni_urovni
Posilovani_odolnosti_vuci_nelegitimnimu_ovlivnovani_ve_vysokoskolskem_a_vyzkumnem_prostredi

ZÁSADA „POZNEJ SVÉHO PARTNERA“

1. **Kdo je** přesně **partnerem**?
2. Kde partner sídlí?
3. Kdo partnera v dané spolupráci reprezentuje?
4. Respektuje partner základní lidská práva a svobody?
5. Uvádí o sobě partner nějaké informace, které nelze jinak doložit?
6. Snaží se partner některé informace o sobě zamlčet?
7. Jak partner spolupracuje s dalšími subjekty (včetně např. řešení sporů)?
8. Podléhá partner kontrole či vlivu nedemokratických režimů?
9. Nepodílí se partner na činnosti, která by byla v ČR považována za protiprávní?
10. Neprovádí partner činnosti, které jsou v ČR považovány za neetické?

Interakce s třetími stranami

Jde zejména o spolupráci v jakékoliv formě spočívající v:

- **pracovních cestách** do,
- **přijímání** zejm. **pracovních návštěv** z,
- **navštěvujících a hostujících akademicích** z,
- **podpisech smluv s právnickými a fyzickými osobami** z,
- **spolupráci** na výzkumných, vzdělávacích, komerčních a dalších projektech a
- **dalších formách spolupráce** s právnickými a fyzickými osobami pocházejícími z anebo majícími
- sídlo či státní příslušnost anebo hájícími zájmy

těch zemí, které jsou **definovány jako vysoce rizikové**.

Vysoce rizikové?

U států, které jsou spojeny s vysokou mírou rizika, **je třeba provést podrobnou due diligence**. Jedná se o následující kategorie států:

- státy uvedené jako rizikové v aktuální **Bezpečnostní strategii ČR**,
- státy, proti nimž nebo proti jejichž státním příslušníkům je vydáno **platné omezující národní opatření** (např. formou usnesení vlády, nařízení vlády, či zákona23),
- všechny státy, vůči jejichž představitelům existují platná **omezující opatření EU** a které jsou
- zároveň uvedené na **EU Sanctions Map**.

VaV (1.1.2027)

Zákon č. 328/2025 Sb., o výzkumu, vývoji, inovacích a transferu znalostí

§ 7 - Institucionální odolnost

(1) **Příjemce institucionální podpory je povinen zajistit** institucionální **odolnost proti vlivovému působení cizí moci**, **kybernetickou a informační bezpečnost** a dodržování předpisů a pravidel týkajících se **ochrany duševního vlastnictví**, mezinárodních kontrolních režimů a mezinárodních sankcí, a to v souladu se zásadou tak otevřeného přístupu k výsledkům, jak je jen možné.

VaV (1.1.2027)

(2) Příjemce institucionální podpory je povinen **zpracovat a naplňovat bezpečnostní a krizovou koncepci**. **Bezpečnostní a krizová koncepce musí zohledňovat rizika související s nelegitimním ovlivňováním v oblasti výzkumu, vývoje, inovací a transferu znalostí**, ochranu bezpečnostních zájmů státu a zájem na rozvoji Evropského výzkumného prostoru.

(3) Bezpečnostní a krizová koncepce, jejíž součástí je **systém řízení rizik**, musí obsahovat

a) **rizika narušení výzkumu, vývoje, inovací a transferu znalostí, a opatření k jejich eliminaci**,

b) **opatření v oblasti kybernetické bezpečnosti**,

c) **opatření v oblasti ochrany výsledků výzkumu, vývoje, inovací a transferu znalostí a údajů z výzkumu v souvislosti s jejich zveřejňováním a ochranou před neoprávněným přístupem k nim nebo nakládání s nimi**,

d) **hodnocení rizik u partnerů v oblasti výzkumu, vývoje, inovací a transferu znalostí** a

e) opatření za účelem rozvoje povědomí o bezpečnosti výzkumu, vývoje, inovací a transferu znalostí, vnitřních hrozbách a o řízení potenciálních rizik spojených s výzkumem, vývojem, inovacemi, transferem znalostí, šířením informací a s výzkumnou spoluprací.

Systém řízení rizik
Opatření

Pro poskytovatele regulované služby v režimu vyšších povinností jsou

Organizační opatření

a) systém řízení bezpečnosti informací,
b) povinnosti vrcholného vedení,
c) bezpečnostní role,
d) řízení bezpečnostní politiky a bezpečnostní dokumentace,
e) řízení aktiv,
f) řízení rizik,
g) řízení dodavatelů,
h) bezpečnost lidských zdrojů,
i) řízení změn,
j) akvizice, vývoj a údržba,
k) řízení přístupu,
l) zvládání kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů,
m) řízení kontinuity činností a
n) audit kybernetické bezpečnosti

Technickými opatření

a) fyzická bezpečnost,
b) bezpečnost komunikačních sítí,
c) správa a ověřování identit,
d) řízení přístupových oprávnění,
e) detekce kybernetických bezpečnostních událostí,
f) zaznamenávání bezpečnostních a relevantních provozních událostí,
g) vyhodnocování kybernetických bezpečnostních událostí,
h) aplikační bezpečnost,
i) kryptografické algoritmy,
j) zajišťování dostupnosti regulované služby a
k) zabezpečení průmyslových, řídicích a obdobných specifických technických aktiv.

Pro poskytovatele regulované služby v režimu nižších povinností jsou bezpečnostními opatřeními

Organizační a technická opatření

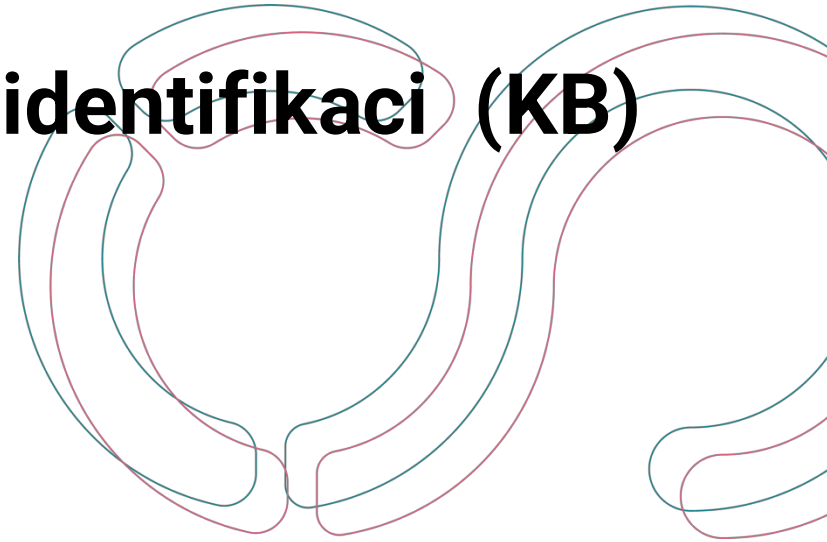
a) systém zajišťování minimální kybernetické bezpečnosti,
b) požadavky na vrcholné vedení,
c) řízení aktiv,
d) řízení rizik,
e) bezpečnost lidských zdrojů,
f) řízení kontinuity činností,
g) řízení přístupu,
h) řízení identit a jejich oprávnění,
i) detekce a zaznamenávání kybernetických bezpečnostních událostí,
j) řešení kybernetických bezpečnostních incidentů,
k) bezpečnost komunikačních sítí,
l) aplikační bezpečnost a
m) kryptografické algoritmy

Propojení KB a due diligence

- **Důvody:**
  - **Povaha aktiv**, které jsou spravovány
  - **Komplexní hrozby**, kterým VaV čelí

- **Využití informací sesbíraných při samoidentifikaci (KB) pro další práci v rámci bezpečnosti VaV**

- **Bezpečnostní a krizová koncepce**

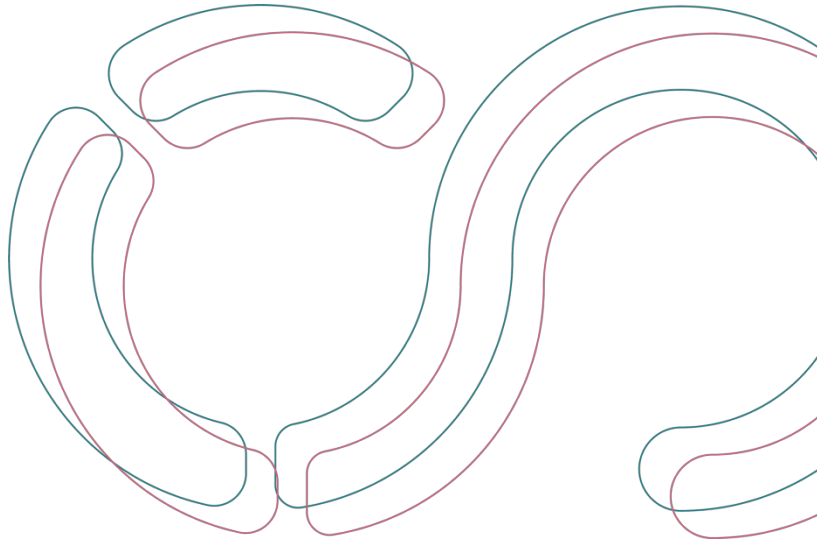


Interakce s třetími stranami

Jde zejména o spolupráci v jakékoliv formě **spočívající v:**

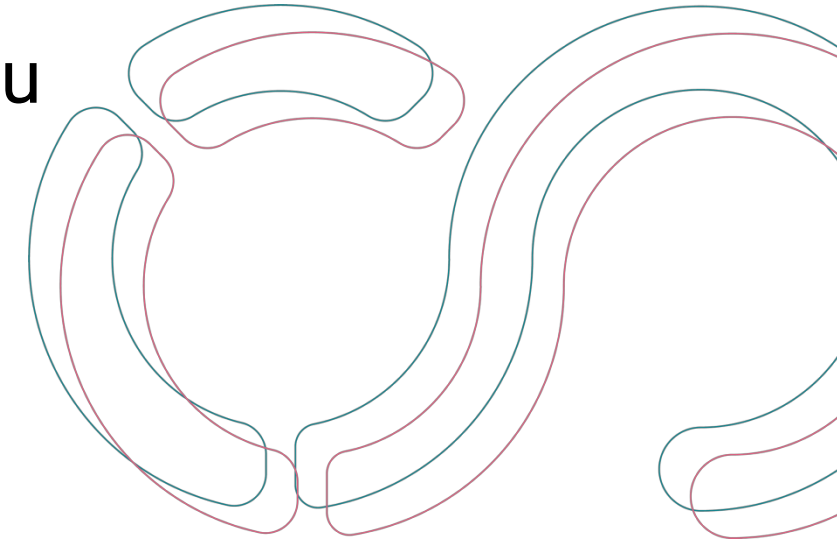
- **spolupráci na výzkumných**, vzdělávacích, komerčních a dalších **projektech** a
- **dalších formách spolupráce** s právnickými a fyzickými osobami…

Game changer?



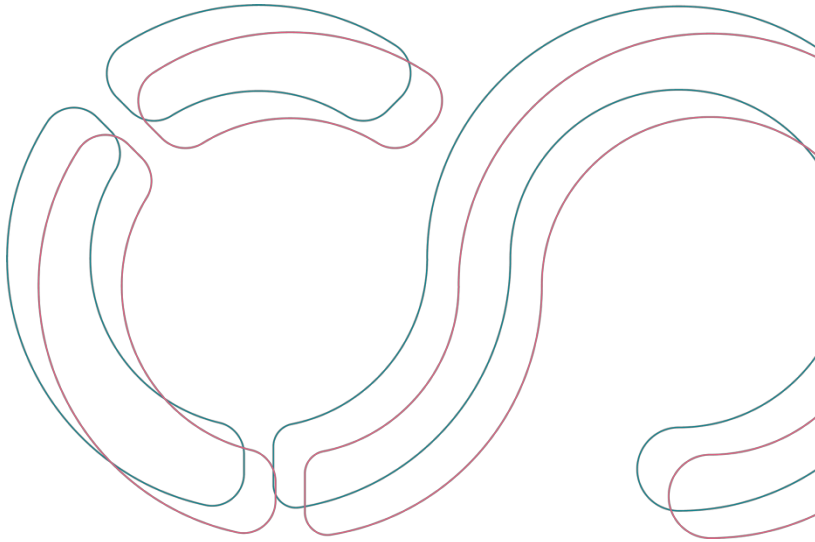
Minulost vs. současnost

- **Žádný** cloud
- **Žádné** repositáře
- **Žádné** instantní a neomezené připojení/propojení
- **Limitované** sdílení informací a výsledků výzkumu



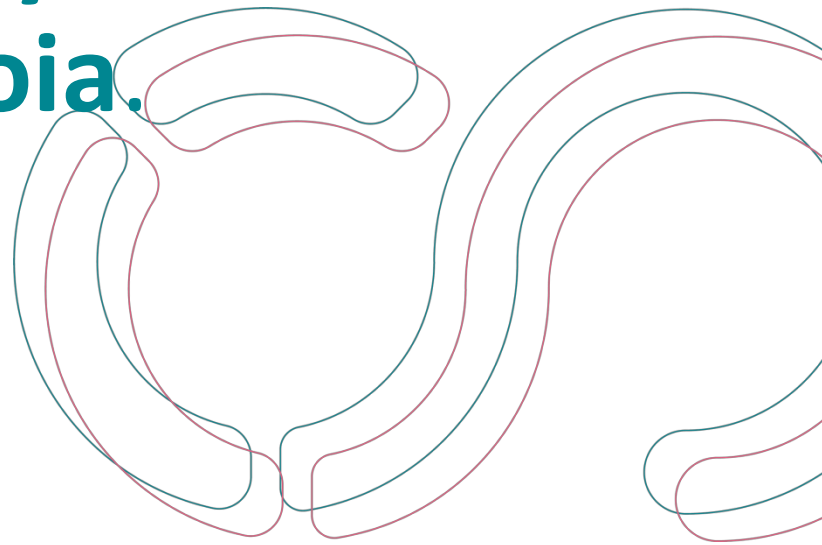
Opened as possible, closed as necessary

- Ochrana dat, informací, infrastruktury
- Ochrana osob (vědců, výzkumníků)
- Ochrana výsledků



Openness vs. security

Research without security – **naivety**.
Security without research – **paranoia**.



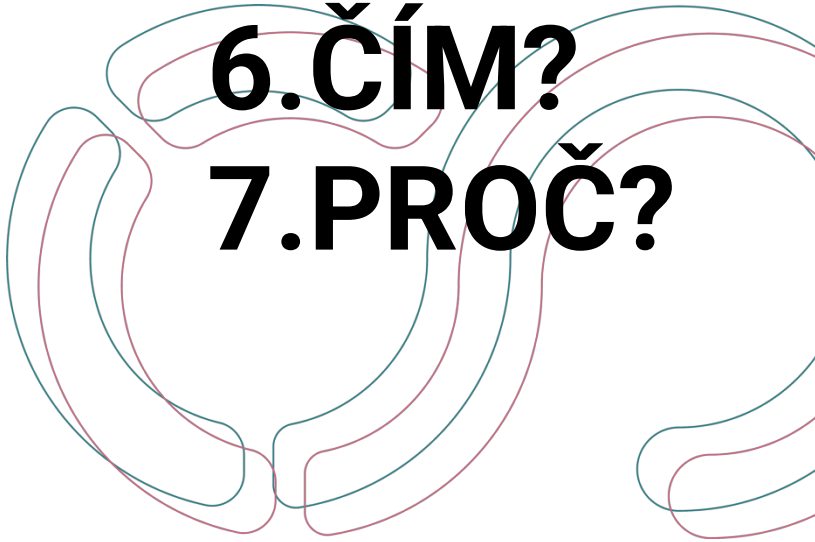
Responsibility!

Každý uživatel!

Analýza rizik

- **Co** sdílíte?
- **S kým**?
- Jaká jsou **pravidla?**
- **Jak** sdílíte?
- Jaká **oprávnění** nastavíte?
- **Jak** zajistíte **bezpečnost**?
- Jaká zvolíte **práva pro užití**?
- **S jakou „podorou“?**

1.CO?
2.KDY?
3.KDE?
4.KDO?
5.JAK?
6.ČÍM?
7.PROČ?



National Czech Programme | eosc

Jak svá aktiva chráníte?

Slido.com

2830447

Jak svá aktiva chráníte?

Review answers 27


TIME TO
PANIC

Je to o nás všech!

National Czech Programme | eosc

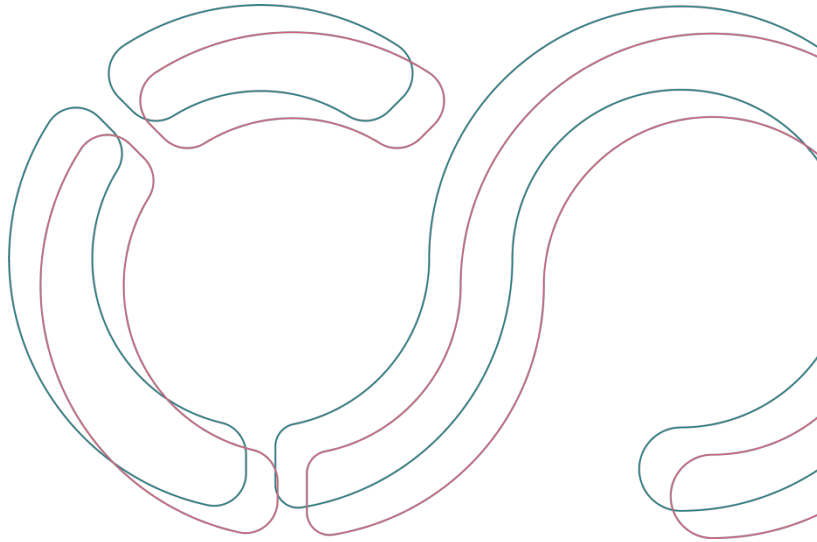
Kultura bezpečnosti ve výzkumu

5E's Framework – NPSA

1. **Educate** why (Informování osob o bezpečnostních hrozbách.)
2. **Enable** how (Umožnit lidem, aby se chovali tak, jak se od nich očekává.)
3. Shape the **environment** (Vytváření prostředí, které lidem usnadní uplatňování požadovaných bezpečnostních postupů.)
4. **Encourage** the action (Poskytování zpětné vazby s cílem podpořit žádoucí chování a odradit od chování nežádoucího.)
5. **Evaluate** the impact (Hodnocení dopadu těchto opatření na bezpečnostní chování osob.)

https://www.npsa.gov.uk/security-best-practices/security-culture/embedding-security-behaviours-using-5es-guidance

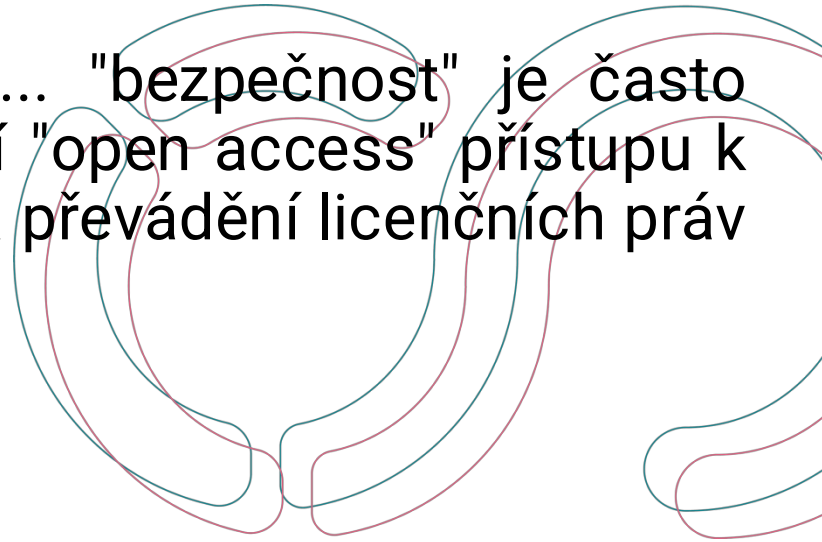
Open science
≠
risky science



Questions?

- Jsou mezi plánovanými opatřeními v NDI např. strategie proti zneužití otevřených dat pro dezinformační kampaně? Jak funguje tzv. tagování dat? A je v NDI v plánu jej zavést?

- vazba na fair principy / "...as open as it possible ... "bezpečnost" je často zmiňovaným (i zástupným) důvodem pro neuplatňování "open access" přístupu k publikacím a jejich zveřejňování pod licencemi "cc-by" a převádění licenčních práv k publikacím na vydavatele důvodem



National Czech Programme | eosc

Partneři

cesnet

MUNI ICS

VŠB TECHNICKÁ UNIVERZITA OSTRAVA | IT4INNOVATIONS NÁRODNÍ SUPERPOČÍTAČOVÉ CENTRUM

UNIVERZITA KARLOVA

Univerzita Palackého v Olomouci

NTK
50°6'14.083"N, 14°23'26.365"E
Národní technická knihovna
National Library of Technology

J. Heyrovský Institute of Physical Chemistry

Středisko společných činností Akademie věd ČR

KNIHOVNA
AKADEMIE VĚD ČR

National Czech Programme | eosc

Děkuji za pozornost

doc. JUDr. Jan Kolouch, Ph.D.

jan.kolouch@cesnet.cz

Spolufinancováno Evropskou unií

Ministerstvo školství, mládeže a tělovýchovy

Registrační číslo projektu NRP

CZ.02.01.01/00/23_014/0008787